شرح عن خدمات NAT&DHCPفي موجهات Cisco

إعداد

عبد الرحمن غسان زعرور

سوريا – حمص – موبايل ٠٩٤٧٦١٥٧٤١

E-mail : Theprince-za08@hotmail.com

تم تطوير Address Translation لحل مشكلتين: قلة العناوين – اخفاء المخطط التفصيلي للشبكة الداخلية

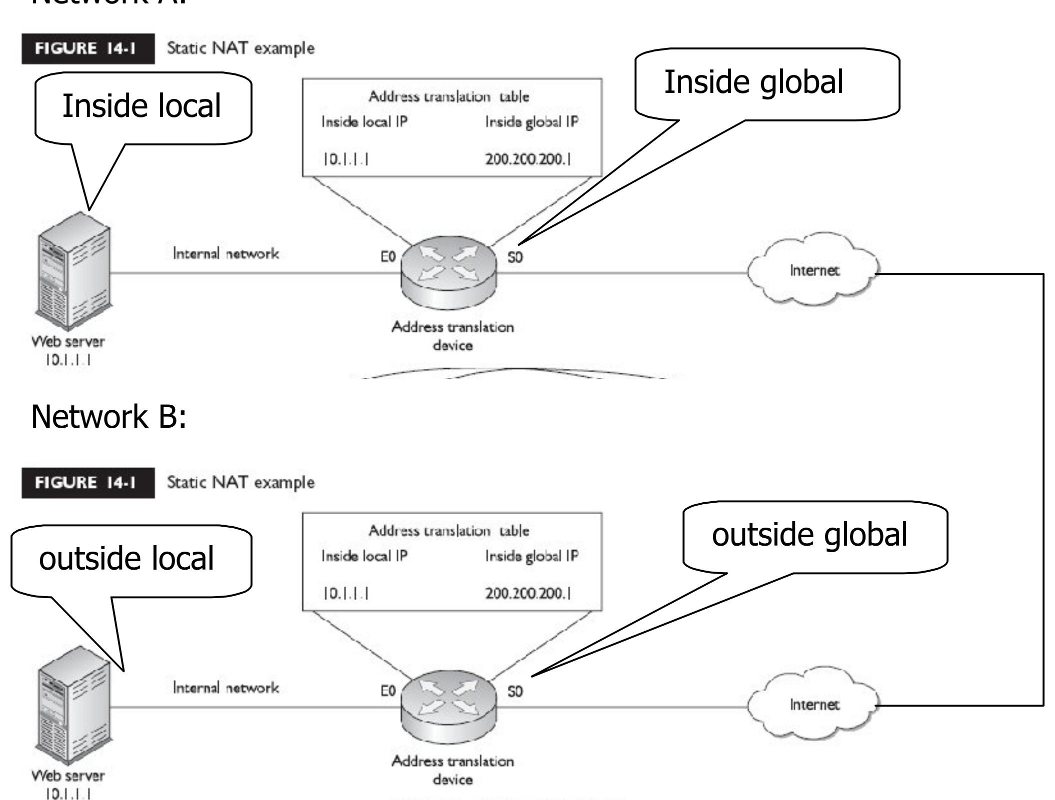
النقاط التالية توضح سبب استخدام Address translation

- استخدام العناوين الخاصة بسبب ان ISP لم يعطيك عنوان عام
- استخدام عناوين عامة وهذه العناوين لا تتواجد مع ISP
- دمج منطقتين تستخدم نفس عناوين الشبكة
- اخفاء الشبكة الداخلية عن الانترنت

بعض النقاط المهمة:

- Inside : الشبكة الموجودة في داخل شبكتك
- Outside : الشبكة الموجود خارج شبكتك
- Local : العنوان الفيزيائي للجهاز
- Global: العنوان العام للجهاز
- Inside local : الجهاز الداخلي في شبكتي الذي يكون عنوانه خاص
- Inside global: الجهاز الداخلي (الـ Router الذي امتلكه) الذي يكون عنوانه عام
- Outside local: الجهاز الخارجي في الشبكة الاخرى الذي يكون عنوانه خاص
- Outside glolbal: الجهاز الخارجي (الـ Router الثاني) الذي يكون عنوانه عام

الرسم التالي يوضح هذه النقاط **بالنسبة** للشبكة A

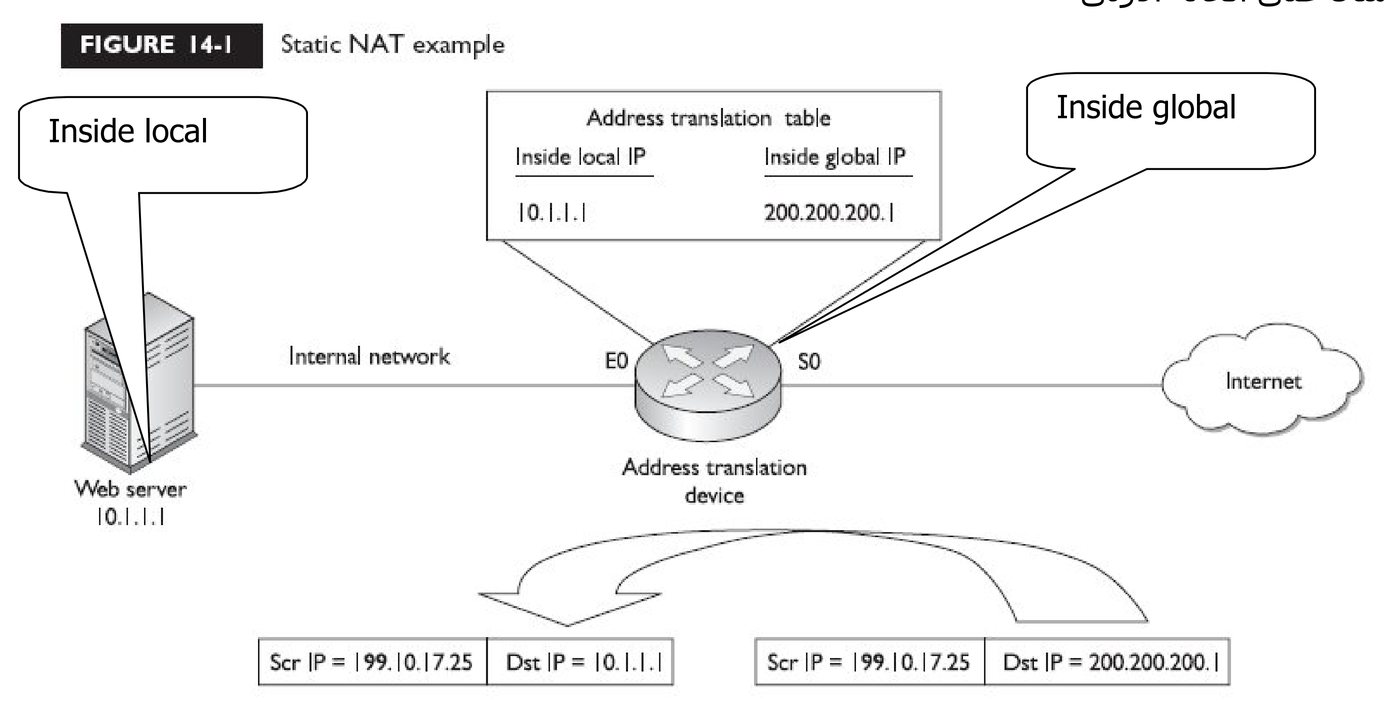


انواع NAT:

اولا: Static NAT

هنا يتم التحويل يدويا من عنوان الى عنوان حيث يمكن ان يتم تحويل عنوان الهدف (المرسل : مستخدم في الانترنت، المستقبل: خادم ويب في الشبكة الداخلية) او تحويل عنوان المرسل (المرسل: مستخدم في الشبكة الداخلية، المستقبل : خادم ويب في الانترنت)

مثال على الحالة الاولى



المرسل: شخص في الانترنت عنوانه ١٩٩,١٠,١٧,٢٥ والمستقبل هو خادم الويب و عنوانه هو ٢٠٠,٢٠٠,٢٠٠,١ ويتم تحويل العنوان ٢٠٠,٢٠٠,٢٠٠,١ الى العنوان الداخلي ١٠,١,١,١ (هنا تم تغير عنوان الهدف فقط)

وهنا نلاحظ انه يجب على مدير الشبكة ان يربط بين العنوان ٢٠٠,٢٠٠,٢٠٠,١ و العنوان ١٠,١,١,١ يدويا باستخدام الاوامر

ثانيا : Dynamic NAT

مع النوع Static يجب ان نبني عملية التحويل يدويا ومع ازدياد عدد الاجهزة تصبح العملية معقدة وتستخدم هذه الطريقة عادة مع مستخدمي الانترنت للوصل الى خادم الويب الموجود فيالشبكة الداخلية

اما مع الحالة الثانية (مستخدموا الشبكة الداخلية يريدون الوصول الى الانترنت) فيفضل استخدام Dynamic NAT

هنا يجب ان نعرف مجموعتين من العناوين :

المجموعة الاولي : العناوين الموجودة في الشبكة الداخلية والتي سوف يسمح لها بالوصول الى الانترنت

المجموعة الثانية : العناوين العامة التي سوف تستخدم في التحويل

طريقة التحويل: عندما يقوم مستخدم داخلي بارسال بيانات عبر Router (جهاز NAT) ، سوف يقوم R بفحص عنوان المرسل ومن ثم مقارنته مع مجموعة العناوين الداخلية (Internal Local address pool) فاذا وجد تطابق فانه يختار بشكل ديناميكي عنوان خارجي من مجموعة العناوين العامة (Inside global address pool) لم يستخدم مع مستخدم آخر

بعد اختيار العناوين المطلوبة تتم اضافتها الى جدول التحويل وبعدها يتم ارسال البيانات الى الانرنت

بعد وصول الرد من الانترنت يتم فحص عنوان المستقبل وفحص هذا العنوان مع جدول التحويل وبعد العثور على هذا العنوان يتم تحويل Global inside address الى local inside address ومن ثم توجيه البيانات الى المستخدم

ثالثا: Port Address Translation (PAT)

في النوعين السابقين عملية التحويل تدعى one to one address translation أي واحد الى واحد ، فاذا كان عدد المستخدمين ١٠٠٠ وكلمه يريد الوصول الى الانترنت بنفس الوقت فإننا نحتاج ١٠٠٠ عنوان عام لذلك لحل هذه المشكلة فاننا نستخدم address overloading وله نوعين PAT و Network Address Port (NAPT) Translation

خدمة PAT :

جميع الاجهزة تستخدم نفس العنوان ولكن نستخدم رقم منفذ المرسل للتميز بين كل مستخدم في الشبكة الداخلية، وفي حال ان كان جهازين يستخدمون نفس رقم المنفذ فان R يغير احد المنافذ

تعمل هذه الخدمة مع بروتوكول TCP و UDP فقط ولكن يوجد دعم لـ ICMP with PAT

رابعا : Port Address Redirection (PAR)

في هذا النوع ندمج بين الحالتين: عندنا خادم ويب داخلي وعندنا مستخدمين في الشبكة الداخلية يريدون الوصول الى الانترنت

ندعوا العملية السابقة بـ **Static PAT**

حيث نجعل عملية **NAT** تبحث عن العنوان العام وعلى رقم منفذ الخدمة الداخلية (٨٠ للويب)

مشاكل **NAT**

بعض البرامج لا تعمل مع هذه الخدمة مثل **Multimedia** و **NetBIOS** – التأخير في معالجة البيانات – يمكن لبعض الهاكر ان يخفي نفسه خلف **NAT**

اعداد Static NAT

اولا : تحديد طريقة التحويل و توجد طريقتين :
الاولى

Router(config)# ip nat inside source static inside_local_source_IP_address inside_global_source_IP_address

هنا مع الكلمة **Inside** يتم تحويل العنوان **inside_local_source_IP_address** الى العنوان **inside_global_source_IP_address**

أي تحويل عنوان المرسل في الشبكة الداخلية الى عنوان عام كمرسل

الثانية:

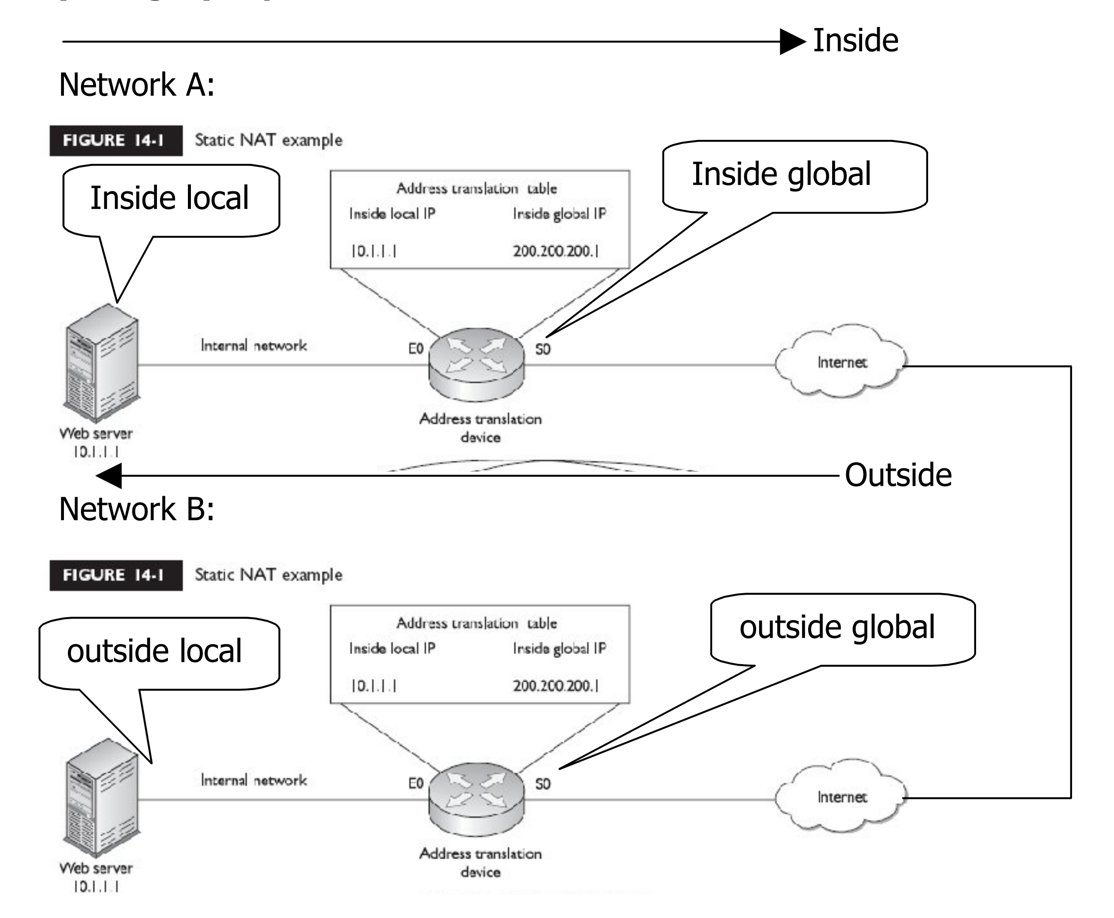
Router(config)# ip nat outside source static outside_global_destination_IP_address outside_local_destination_IP_address

هنا مع الكلمة **Outside** يتم تحويل **outside_global_destination_IP_address** الى العنوان **outside_local_destination_IP_address**

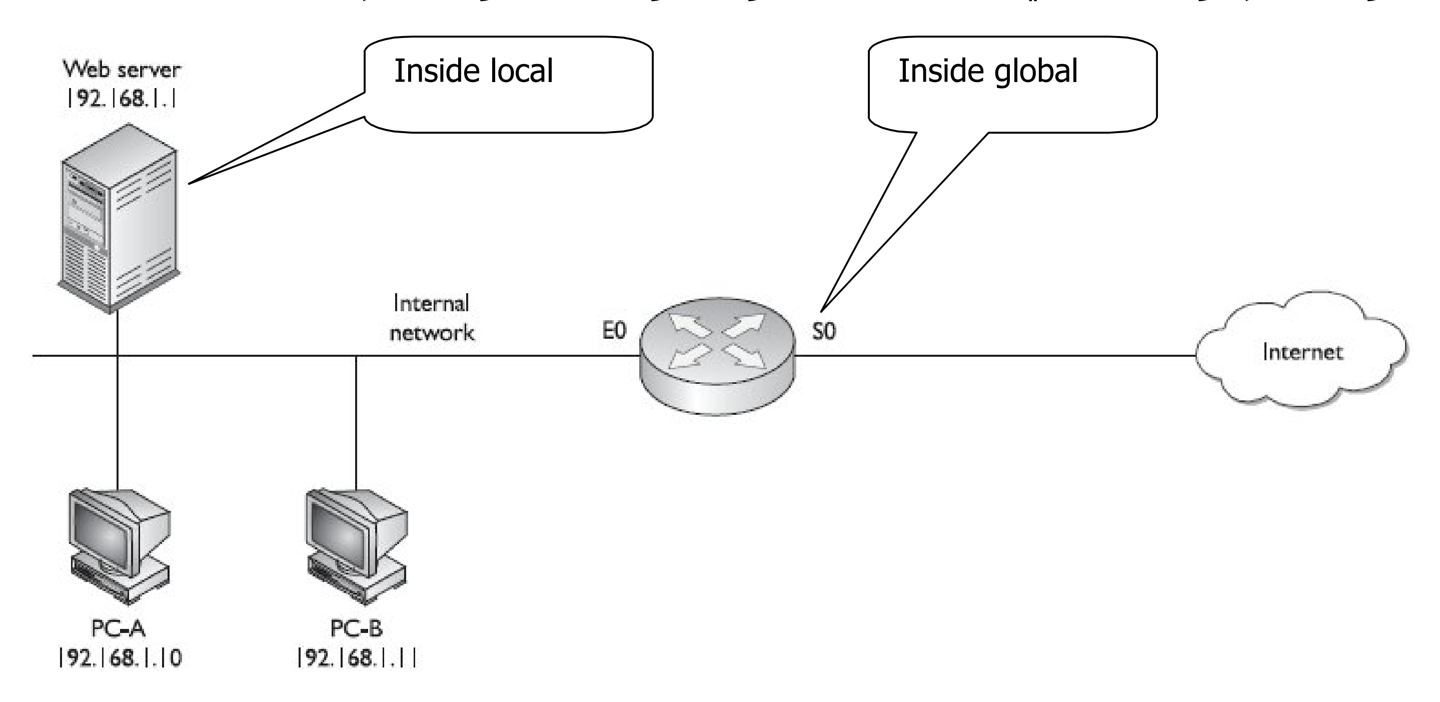
أي تحويل عنوان الهدف العام للراوتر الى عنوان خاص في الشبكة الداخلية

ثانيا : تحديد الوصلة هل هي **Inside** او **outside**

Router(config)# interface type [slot_#/]port_#
Router(config-if)# ip nat inside|outside



مثال
عنوان خادم الويب الداخلي **192.168.1.1** سوف يحول الى العنوان العام **200.200.200.1**



الاوامر

```
Router(config)# ip nat inside source static   192.168.1.1     200.200.200.1
Router(config)# interface ethernet 0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface serial 0
Router(config-if)# ip nat outside
Router(config-if)# exit
```

ملاحظة : هنا لا نحتاج الى تعريف POOL ولا لـ ACL

اعداد Dynamic NAT

هنا يجب ان نحدد ثلاث نقاط :

١- العناوين الداخلية التي يجب ان تحول
٢- العناوين العامة التي سوف تستخدم في التحويل
٣- الوصلات المستخدمة في التحويل

اولا: تحديد العناوين الداخلية يتم بالامر:

En
Config t
IP NAT Inside Source List *standard_ip_acl* **Pool** *pool_name*

Standard_ip_acl : تستخدم لتحديد العناوين الداخلية، أي عنوان يذكر مع **Permit** سوف يسمح له بالتحويل واي عنوان يذكر مع **deny** او لم يذكر فانه يمنع من التحويل

ثانيا: تحديد العناوين العامة بالامر:

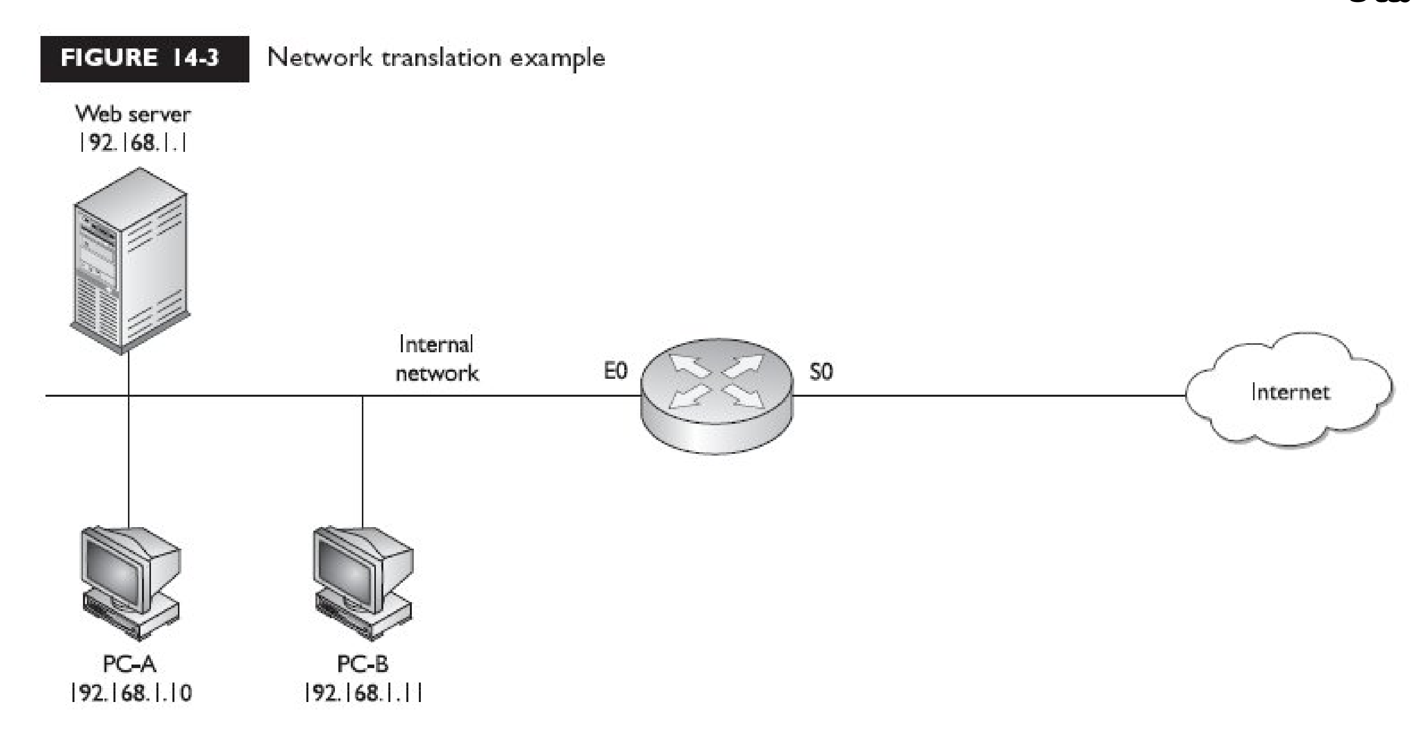
En
Config t
IP NAT Pool *pool_name* *begin_inside_global_ip* *ending_inside_global_ip* **netmask** *subnet*

ثالثا: تحديد الوصلات المستخدمة في التحويل بالامر:

En
Config t
Int E0
IP NAT Inside
Int S0
IP NAT Outside

ملاحظة: عدد العناوين العامة يجب ان تكون اكبر من او يساوي عدد العناوين في الشبكة الداخلية

مثال



الاوامر

Router> En
Router# Config t

الخطوة الاولى

Router(config)# ip nat inside source list 1 **pool** nat-pool
Router(config)# access-list 1 permit 192.168.1.10 0.0.0.0
Router(config)# access-list 1 permit 192.168.1.11 0.0.0.0

الخطوة الثانية

Router(config)# ip nat pool nat-pool 200.200.200.2 200.200.200.3 netmask 255.255.255.0

الخطوة الثالثة

Router(config)# interface ethernet 0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface serial 0
Router(config-if)# ip nat outside
Router(config-if)# Ctrl + Z
Router#

اعداد PAT

تتم على ثلاث مراحل:
١- تحديد العناوين الداخلية التي سوف تحول
٢- تحديد العناوين العامة المستخدمة في التحويل
٣- الوصلات المستخدمة في التحويل

اولا : تحديد العناوين الداخلية بالامر

En
Config t
IP NAT Inside Source List *standard_ip_acl* **Pool** *pool_name* **overload**

Standard_ip_acl : تستخدم لتحديد العناوين الداخلية، أي عنوان يذكر مع **Permit** سوف يسمح له بالتحويل واي عنوان يذكر مع **deny** او لم يذكر فانه يمنع من التحويل

ثانيا: العناوين العامة

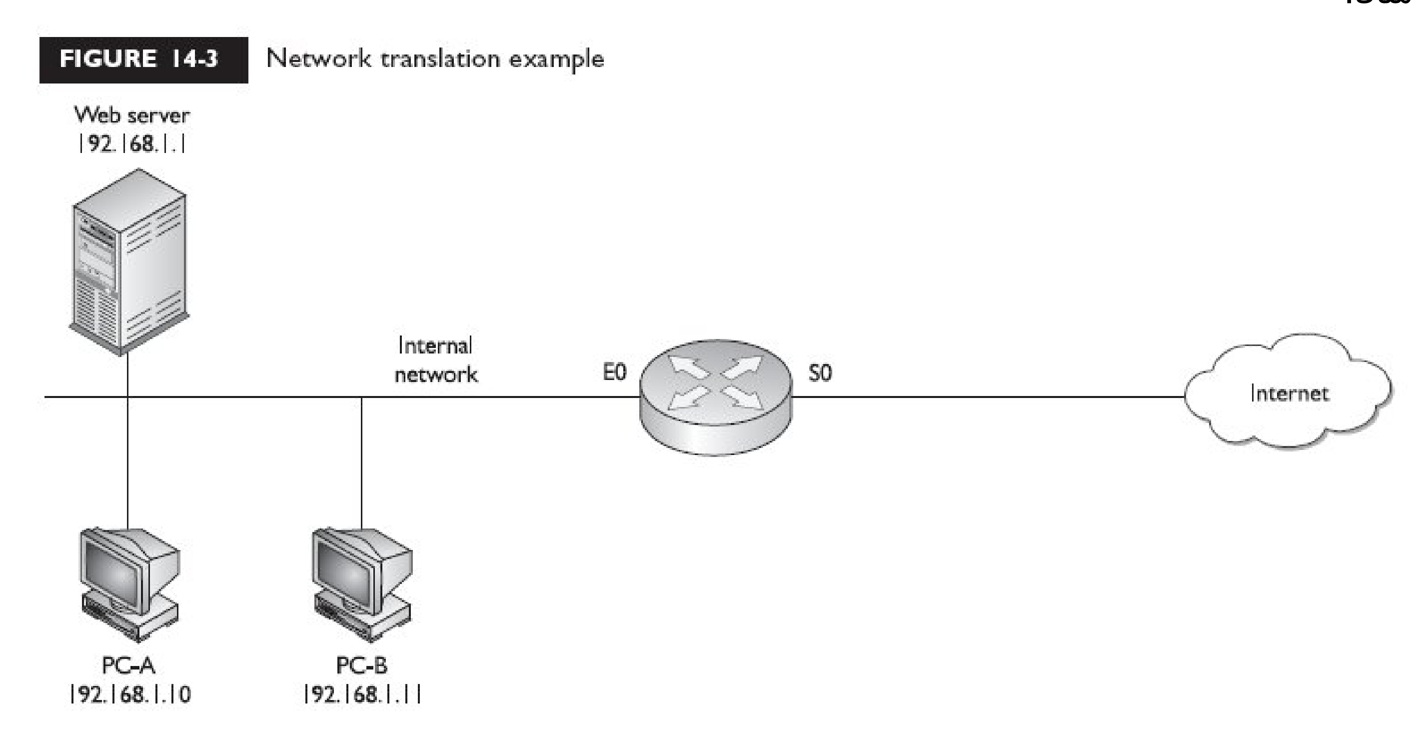
En
Config t
IP NAT Pool *pool_name* *begin_inside_global_ip* *ending_inside_global_ip* **netmask** *subnet*

ملاحظة: هنا يمكن ان نحدد اكثر من عنوان في المجال او يمكن ان نحدد عنوان واحد فقط

ثالثا: تحديد الوصلات المستخدمة في التحويل بالامر:

En
Config t
Int E0
IP NAT Inside
Int S0
IP NAT Outside

مثال:



Router> En
Router# Config t

الخطوة الاولى

Router(config)# ip nat inside source list 1 pool nat-pool overload
Router(config)# access-list 1 permit 192.168.1.10 0.0.0.0
Router(config)# access-list 1 permit 192.168.1.11 0.0.0.0

الخطوة الثانية

Router(config)# ip nat pool nat-pool 200.200.200.2 200.200.200.2 netmask 255.255.255.0

الخطوة الثالثة

Router(config)# interface ethernet 0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface serial 0
Router(config-if)# ip nat outside

هنا استخدمنا عنوان واحد فقط 200.200.200.2 للتحويل مع الجهازين PC-A & PC-B

توزيع الحمل

يستطع جهاز router توزيع الطلبات التي تأتي الى عنوان واحد عام لكي تحول الى عدة عناوين في الشبكة الخاصة

فمثلا : لدينا خادمين ويب بنفس المحتوى ونريد تقسيم الطلبات الواردة على هذين الخادمين

فمع NAT سوف نجري عملية Round robin ضمن العناوين الداخلية ولكن لدينا مشكلة: لا يمكن ان نعرف اذا كانت الخدمة فعالة عند ارسال الطلب اليها

الخطوات:

١- تحديد العناوين الدخلية للخدمات

٢- تحديد العناوين الخارجية

٣- تحديد الوصلات المستخدمة

الاول: تحديد العناوين الداخلية يتم بالاوامر التالية

Router(config)# ip nat pool *pool_name beginning_inside_local_IP_address*

ending_inside_local_IP_address **prefix-length** *subnet_mask_bits* **type rotary**

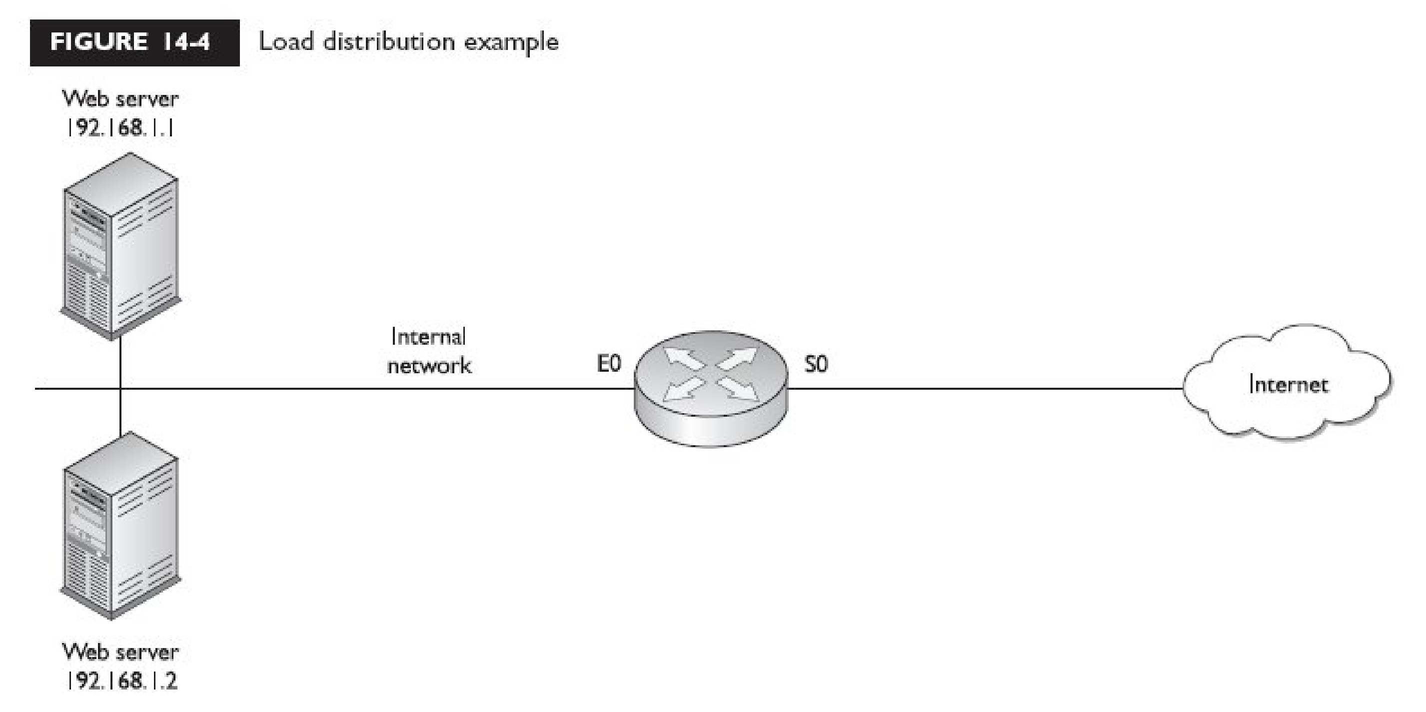
حيث نحدد اول عنوان وآخر عنوان في الشبكة الداخلية للأجهزة التي عليها الخدمات ثم نحدد عدد خانات القناع ثم كلمة **Type rotary** لكي تبدأ عملية round robin

ثانيا : تحديد العناوين الخارجية (العامة)

Router(config)# ip nat inside destination list *standard_ACL_#* **pool** *pool_name*

ثالثا: نستخدم الاوامر مع الوصلات : **IP NAT Inside** و **IP NAT Outside**

مثال:



الاوامر

En

Config t

الخطوة الاولى

Router(config)# ip nat pool *inside-hosts* **192.168.1.1 192.168.1.2 prefix-length 24 type rotary**

الخطوة الثانية

Router(config)# ip nat inside destination list 1 pool *inside-hosts*

Router(config)# access-list 1 permit 200.200.200.1

الخطوة الثالثة

Router(config)# interface ethernet 0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface serial 0
Router(config-if)# ip nat outside
Exit

الامر التالي يستخدم لعرض عمليات التحويل Show Ip NAT translations

مثال

Router# show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	200.200.200.1	192.168.1.1	---	---
---	200.200.200.2	192.168.1.2	---	---

هنا نلاحظ ان العملية هي **NAT** حيث يحول العنوان ١٩٢,١٦٨,١,١ الى ٢٠٠,٢٠٠,٢٠٠,١

مثال

Router# show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
tcp	200.200.200.1:1080	192.168.1.1:1080	201.1.1.1:23	201.1.1.1:23
tcp	200.200.200.1:1081	192.168.1.2:1080	201.1.1.1:23	201.1.1.1:23

هنا النوع هو PAT حيث نلاحظ ان الجهازين ١٩٢,١٦٨,١,١ و ١٩٢,١٦٨,١,٢ يحاولان الوصول الى ٢٠١,١,١,١ باستخدام البروتوكول Telnet (رقم المنفذ ٢٣)

الامر التالي **show ip nat statistics** يعرض بعض الارقام

Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet0

Hits: 98 Misses: 4
Expired translations: 1

Hits عدد مرات التطابق و **Miss** عدد مرات عدد التطابق

Dynamic mappings:
-- Inside Source
access-list 1 pool nat-pool refcount 2
pool nat-pool: netmask 255.255.255.255
start 200.200.200.10 end 200.200.200.254
type generic, total addresses 12, allocated 1 (9%), misses 0

مسح الجداول

Router# **clear ip nat translation ***
Router# **clear ip nat translation inside** global_IP_address local_IP_address
Router# **clear ip nat translation outside** global_IP_address local_IP_address
Router# **clear ip nat translation** protocol **inside** global_IP_address global_port local_IP_address local_port

عملية **Debug**

Router# debug ip nat
05:32:23: NAT: s=192.168.1.10->200.200.200.2, d=201.1.1.1 [70]
05:32:23: NAT*: s=201.1.1.1, d=200.200.200.2->192.168.1.10 [70]

السطر الاول يبين ان المرسل هو ١٩٢,١٦٨,١,١٠ وتم تحويل العنوان الى ٢٠٠,٢٠٠,٢٠٠,٢
وهذا العنوان يرسل الى جهاز في الانرنت عنوانه ٢٠١,١,١,١
السطر الثاني يبين عملية الرد من ٢٠١,١,١,١ باتجاه ٢٠٠,٢٠٠,٢٠٠,٢ ومن ثم الى
١٩٢,١٦٨,١,١٠

خدمة DHCP

Router(config)# [no] service dhcp
Router(config)# ip dhcp pool *pool_name*
Router(config-dhcp)# network *network_number [subnet_mask | /prefix_length]*
Router(config-dhcp)# domain-name *domain_name*
Router(config-dhcp)# dns-server *IP_address [IP_address_2...IP_address_8]*
Router(config-dhcp)# netbios-name-server *IP_address [IP_address_2...IP_address_8]*
Router(config-dhcp)# netbios-node-type *node_type*

These types can be **b** (broadcast only), **p** (WINS only), **m** (broadcast, then WINS), or **h** (WINS, then broadcast)

Router(config-dhcp)# default-router *IP_address [IP_address_2...IP_address_8]*
Router(config-dhcp)# lease *days [hours][minutes]* | **infinite**
Router(config-dhcp)# exit
Router(config)# ip dhcp ping timeout *milliseconds*

By default, this is 500 milliseconds. If the server doesn't receive a reply in this time period, the server will assume the address is not being used and offer this to the client.

Router(config)# ip dhcp excluded-address *beginning_IP_address [ending_IP_address]*

الامر التالي يجعل الـ **Router** جهاز **DHCP client**

Router(config)# interface type [slot_#/]port_#
Router(config-if)# ip address dhcp

الامر التالي يستخدم لعرض العناوين التي وزعت

show ip dhcp binding [client_address]

لمسح جدول التوزيع

clear ip dhcp binding client_address | *

لعرض العنوان الذي اخذته من **DHCP Server**

show ip interface brief
show interfaces

لعرض **Debug**

debug ip dhcp server events|packet|linkage